



A Community of Friends. A World of Opportunities.

280 Saunders Road, Riverwoods, Illinois 60015-3835
p: 847.948.7001 • f: 847.948.7621 www.CenterForEnrichedLiving.org

August 4, 2020

The Honorable Wayne Stenehjem
Attorney General of the State of North Dakota
600 E. Boulevard Ave. Dept. 125
Bismarck, ND 58505

Dear Attorney General Stenehjem:

I am writing you pursuant to N.D.C.C. 51-30-02 to notify you of a breach of data security involving one North Dakota resident, and 1071 total individuals.

On July 16th, 2020 we received notice from Blackbaud, one of our third-party service providers, of a security incident. A copy of that notice is enclosed as Exhibit A. We understand that Blackbaud discovered and stopped a ransomware attack. After discovering the attack, Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their system access and fully encrypting files, and they ultimately expelled the cybercriminal from their system. Prior to getting locked out of the system, however, the cybercriminal removed a copy of our backup file containing the name and date of birth of one North Dakota resident. The file also contained personal information, as defined by relevant state law, of 1071 total individuals, the majority of whom are residents of Illinois.

According to Blackbaud, the breach occurred at some point between February 7, 2020 and May 20, 2020. Blackbaud has posted additional information about the incident on its website at <https://www.blackbaud.com/securityincident>. Based on the information we have received from Blackbaud, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made publicly available.

In response to Blackbaud's notice to us, we are in turn providing notice to the individuals whose personal information was potentially compromised. A copy of the notification template is enclosed as Exhibit B. The notification letters will be mailed no later than August 15th, 2020.

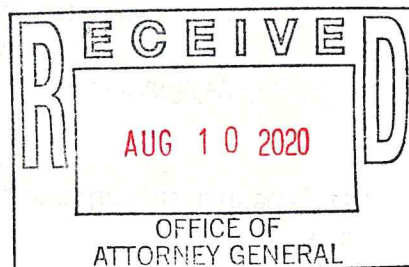
If you have any questions, please contact me by phone at (847) 948-7001, by mail at 280 Saunders Rd., Riverwoods, IL 60015, or by email at Harriet@CenterforEnrichedLiving.org.

Sincerely,

A handwritten signature in cursive script, appearing to read 'Harriet'.

Harriet Levy
CEO
Center for Enriched Living

Enclosures



201894

Rachael Krulewich

From: Nichols Condon <nichols.condon@blackbaud.com>
Sent: Thursday, July 16, 2020 10:44 AM
To: Rachael Krulewich
Subject: Notification of Security Incident

blackbaud®

Dear Rachael,

Please see a personalized note below for your organization from our Chief Information Officer. Thank you.

Dear Rachael,

We are writing to notify you about a particular security incident that recently occurred. Please review this email for a personalized link, next steps and resources created for your organization specifically.

What Happened

The Cybercrime industry represents an over trillion-dollar industry that is ever-changing and growing all the time—a threat to all companies around the world. At Blackbaud, our Cyber Security team successfully defends against millions of attacks each month and is constantly studying the landscape to ensure we are able to stay ahead of this sophisticated criminal industry. **In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attempted attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system.**

Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. The cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data was our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.

Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. In accordance with regulatory requirements and in an abundance of caution, we are notifying all organizations whose data was part of this incident and are providing resources and tools to help them assess this incident.

What This Means for Your Organization Specifically

Our public cloud environment (Microsoft Azure and Amazon Web Services) and most of our self-hosted datacenters, products and customers were not part of this incident, but we have confirmed the following specific to your organization:

- A copy of your Blackbaud NetCommunity, Blackbaud Raiser's Edge NXT, and ResearchPoint backup was part of this incident. Again, the file the cybercriminal removed a copy of did not contain any credit card information. Further, the cybercriminal did not gain access to bank account information, usernames, passwords, or social security numbers stored in your database because they were encrypted. None of your data was lost or corrupted as a result of this incident.

And again, based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. We have hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

We have created a [resource page](http://www.blackbaud.com/incidentresources) for you at www.blackbaud.com/incidentresources that features a toolkit with a step-by-step guide to help you as you digest this information. It also contains answers to key questions, links to educational webinars (hosted by Rich Friedberg, Blackbaud's Chief Information Security Officer and Cameron Stoll, our Head of Privacy), information about our future plans, and other resources.

It is unlikely but possible, depending on jurisdiction, that our customers may have to make further notifications to constituents or other third parties. Your toolkit provides a written guide to notification laws and access to a webinar that helps you assess potential notification requirements in your jurisdictions. We advise you to also consult with your organization's legal counsel to understand any notification requirements. We want to continue to be your partner through this incident. If you determine that you do need to notify your constituents, we have included templates in your toolkit to make it easier.

To ensure all your questions are answered as quickly as possible, we encourage you to first review the resources we provided at the link above. If you still have questions after reviewing these resources, we are here to help. Please contact the dedicated team we have established for this incident:

- **North and South America:** 1-855-907-2099 between 9 a.m. and 9 p.m. ET Monday – Friday

We understand this situation is frustrating. This was a very sophisticated attack, and while we were able to defend against it for the most part, we realize this is still requiring that you invest time to review the situation, and that you may need to invest time to take follow-up actions. We apologize for this and will continue to do our very best to supply help and support as we and our customers jointly navigate any necessary response to the cybercriminal's actions.

Sincerely,

Todd Lant
Chief Information Officer



Please add nichols.condon@blackbaud.com to your address book or safe senders list.

[Manage your subscription preferences.](#)

Date: [DATE OF NOTICE]

NOTICE OF DATA BREACH

Dear [Individual Name]:

We are writing to notify you about a data security incident that may have involved your personal information.

1. What Happened?

We were recently notified by Blackbaud, one of our third-party service providers, of a security incident involving Blackbaud's systems. We understand that Blackbaud discovered and stopped a ransomware attack. After discovering the attack, Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their system access and fully encrypting files, and they ultimately expelled the cybercriminal from their system. Prior to getting locked out of the system, however, the cybercriminal removed a copy of our backup file containing your personal information. This occurred at some point between February 7, 2020 and May 20, 2020.

2. What Information Was Involved?

The cybercriminal did not access any credit card information, bank account information, or social security numbers. However, we have determined that the file removed contained certain medical information and birth dates for certain individuals. It is our understanding that Blackbaud paid the cybercriminal's ransom demand and the cybercriminal confirmed that the copy of the file had been destroyed. **Based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly.**

3. What We Are Doing.

Given the circumstances of the breach and the nature of the compromised information, we do not have reason to believe that the incident will result in identity theft or fraud. Nonetheless, we are notifying you so that you can protect yourself.

Moreover, as part of their ongoing efforts to help prevent something like this from happening in the future, Blackbaud has already implemented several changes that will protect your data from any subsequent incidents. First, Blackbaud's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. Additionally, they are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms. You can get more information by visiting Blackbaud's website at <https://www.blackbaud.com/securityincident>.

4. What You Can Do.

Again, the information that was accessed by the cybercriminal did not include credit card information, bank account information, or social security number. We therefore do not have reason to believe that the incident will result in identity theft or fraud. There, however, are steps that you can take to protect against identity theft and fraud should you choose to do so.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

Report Incidents. Remain vigilant and monitor your account statements. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Place an initial fraud alert.
- Order your credit reports.
- Create an FTC Identity Theft Affidavit by submitting a report about the theft at <http://www.ftc.gov/complaint> or by calling the FTC.
- File a police report about the identity theft and get a copy of the police report or the report number. Bring your FTC Identity Theft Affidavit with you when you file the police report.
- Your Identity Theft Report is your FTC Identity Theft Affidavit plus your police report. You may be able to use your Identity Theft Report to remove fraudulent information from your credit report, prevent companies from refurnishing fraudulent information to a consumer reporting agency, stop a company from collecting a debt that resulted from identity theft, place an extended seven-year fraud alert with consumer reporting agencies, and obtain information from companies about accounts the identity thief opened or misused.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Obtain A Security Freeze You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and

services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. See below for more details on placing a fraud alert on your credit file.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

Placing, temporarily lifting, and removing a security freeze (also known as a "credit freeze") is free of charge. To place, temporarily lift, or remove a security freeze on/from your credit file, you must make a request with each of the three nationwide consumer reporting agency individually. For more information on security freezes, you may contact the three nationwide consumer reporting agencies as described below or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

Place a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to

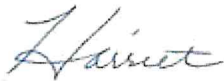
flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285 (Fraud Alert) 1-800-349-9960 (Credit Freeze)	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289 (Fraud Alert) 1-888-909-8872 (Credit Freeze)	www.transunion.com

For More Information.

We sincerely regret any inconvenience this may cause you. If you have any additional questions or concerns, please contact me by phone at (847) 948-7001, by mail at 280 Saunders Rd., Riverwoods, IL 60015, or by email at Harriet@CenterforEnrichedLiving.org.

Sincerely,



Harriet Levy
CEO

